UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,884	03/03/2000	George Fleming	US008002	5479

7590 10/27/2003

U S Philips Corporation
Corporate Patent Counsel
580 White Plains Rd
Tarrytown, NY 10591

EXAMINER
ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
09/517,884	FLEMING ET AL.
Examiner	**Art Unit**
Mossadeq Zia	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 9/8/2003 .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Claim Objections

1. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Numbering of claim 15 is listed twice. Misnumbered claim 15 and 16 has been subsequently renumbered to read 16 and 17.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-3, 5, 7, 12-14, and 16 are rejected under 35 U.S.C. 102(b) as anticipated by U.S. Patent No. 5,148,481, Abraham et al.

4. Regarding claim 1, Abraham et al discloses a processing system comprising:

an application device (workstation) (Abraham, fig. 3, label 25) that is configured to communicate information with a physical-layer (I/O) (Abraham, fig. 2, label 43) access device via a link-layer (RS-232) (Abraham, fig. 3, label 61) access device, a node controller (cryptographic adapter) that is configured to control the link-layer access device (Abraham, fig. 4, col. 3, line 50-52),

the link-layer access device (IC card reader) (Abraham, fig. 2, label 19, 67), operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device (Abraham, fig. 2, label 53, 25, col. 6 line56-60);

wherein, the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller (Abraham, col. 6, line 37-40).

5. Regarding claim 2 and 3, Abraham et al discloses the processing system of claim 1, wherein the one or more cryptographic items include at least one of:

a digital signature (Abraham fig. 14, label 337),

a verification of a digital signature (Abraham fig. 14, label 341), and

a cryptographic key item (Abraham, col. 6, line 65-68).

7. Regarding claim 5, Abraham et al discloses the processing system of claim 1, wherein the node controller (cryptographic adapter) is configured to effect an "exchange of a cryptographic key" (session key) with an other processing system, and the one or more cryptographic items from the link-layer access device includes the cryptographic key (Abraham, col. 14, line 15-20, fig. 14, label 329).

8. Regarding claim 7, Abraham et al discloses a link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device (Abraham, fig. 1, label 13, 23, 25),

a physical-layer interface device that is configured to communicate data with a physicals layer device (Abraham, fig. 1, label 13, 23, 25),

a buffer device (Abraham, fig. 3, label 67), operably coupled to the application-layer interface device and the physical-layer interface device (Abraham, fig. 3, label 53), that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device (Abraham, fig. 4, label 83, col. 6, line 37-40),

a controller interface device (Abraham, fig. 4, label 97), operably coupled to the application-layer interface device (Abraham, fig. 4, label 93) and the physical-layer interface device (Abraham, fig. 4, label RS-232), that is configured to facilitate control of the exchange of information and data, and (Abraham, col. 6, line 37-40)

an accelerator (encryption processor) (Abraham, fig. 4, label 85), operably coupled to a controller via the controller interface device (Abraham, fig. 1, label 29), that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller (Abraham, fig. 12, col. 12, line 66-67), and to thereafter communicate the one or more cryptographic items to the controller (Abraham, col. 7, line 35-38).

9. Regarding claim 12, Abraham et al discloses a method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device (Abraham, fig. 1, label 13, 23, 25), controlling the link-layer access device (Abraham, fig. 3, label RS-232, 97, 99), in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device (Abraham, fig. 14, label 325, 327, 329), and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller (Abraham, fig. 14, 337).

10. Regarding claim 13 and 14, see claim 2 and 3 where it restates the subject matter with similar language.

11. Regarding claim 16, Abraham et al discloses the method of claim 12, and further including effecting an exchange of a cryptographic key with an other processing system, wherein the one or more cryptographic items from the link-layer access device includes the cryptographic key (Abraham, fig. 13).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 4, 6, 8-10, 11, 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,148,481, Abraham et al as applied to claims 1, 7, 12 above, and further in view of "Design and Implementation of Arithmetic Processor F_2^{155} for Elliptic Curve Cryptosystems" by Sutikno et al.

14. Regarding claim 4, 8, and 15, Abraham et al discloses the processing system of claim 1, wherein the link-layer access device (IC card and reader) (Abraham, fig. 2, label 17, 19) but fail to show that it includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others. Sutikno also teaches deriving a second point from the first point on the elliptic curve is a function in ECC (Sutikno, col. 2, line 18, specifically the equation) from inputs (one or more of the parameters) (Sutikno, col. 5, lines 30-33) and where the Main Controller controls all the process to the of the arithmetic processor (Sutikno, col. 7, line 7-9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card (link-layer access device) applications (Sutikno, col. 8, line 8-10).

15. Regarding claim 6, 11, and 17, Abraham et al discloses the processing system of claim 1 however fail to show that the commands from the node controller include:

a basepoint multiply command,

a point multiply command,

an EC-DSA verify command, and

an EC-DSA sign command.

In regards to multiply commands and EC-DSA commands, Sutikno Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card (link-layer access device) applications (Sutikno, col. 8, line 8-10).

16. Regarding claim 9 and 10, Abraham et al discloses the link-layer access device of claim 7, wherein the one or more cryptographic items includes at least one of:

a signature of a message (Abraham, fig. 14, label 337),

a verification of a digital signature (Abraham, fig. 14, label 341),

a hash of one or more parameters (message authentication code) (Abraham col. 7, line 40),

a random number (Abraham fig. 14, label 331),

however, Abraham fail to disclose

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters, the one or more parameters being provided by the controller.

In regards to elliptic curve multiplication of one or more parameters, Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others.

In regards to exponentiation of one or more parameters, Sutikno teaches that squaring (exponentiation) can be accomplished by a simple rotation of the vector representation by using cyclical shift register and the operation only requires one clock cycle (Sutikno, col. 4, line 46-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno because the technique allows elliptic curve multiplication (arithmetic operation) to be easily performed (Sutikno, col. 4, line 27-28).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is (703)305-8425. The examiner can normally be reached on Monday thru Friday between 8:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (703)308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

Mz
09/12/2003

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134